

CA Assembly Bill 655: 1/1/02. Allows consumers and ID theft victims to stop credit bureaus from selling or giving their names to companies that solicit credit cards, block certain credit information, and delete fraudulent credit inquiries from their records.

CA Senate Bill 125: 1/1/02. Allows ID theft victims to obtain copies of all fraudulent applications submitted to credit companies using their names and personal information.

CA Senate Bill 168: 7/1/02. Restricts use of Social Security Numbers as identifiers for access to products or services. 1/1/03: If requested by consumer, requires consumer credit agencies to place a security freeze on the release of information.

CA Senate Bill 1254: 8/24/02. Expands definition of personal information to strengthen existing laws and punishments for identity theft. Personal identifying information now includes name, address, phone number, health insurance ID number, driver's license or ID card number, SSN, place of employment, employee ID, mother's maiden name, account number (savings, checking, demand deposit, or credit card), alien registration number, passport number, date of birth, biometric data (fingerprints, retina or iris scans, voice prints, facial scans, etc.), and birth and death certificates.

Senate Bill 1239: 7/1/03. Upon the consumer's request, consumer credit reporting agencies must provide a statement describing the statutory right of identity theft victims, and provide one free copy of the victim's credit file each month, for up to twelve consecutive months.



Visit www.leginfo.ca.gov for California consumer protection laws and future legislation. Click on Bill Information, and search the key words "consumer protection" or "identity theft."

Visit www.calstatela.edu/its/policies for relevant information privacy and protection legislation links.

Family Educational Rights and Privacy Act (FERPA): Federal law that protects the privacy of student education records. Parents or eligible students (18 years of age) have the right to inspect education records and to request corrections if inaccurate or misleading. Generally schools cannot release any education record without written permission from the parent or eligible student. Under certain conditions some records can be disclosed without consent to or for: accrediting organizations, schools to which a student is transferring, judicial orders or subpoenas, health and safety emergencies. If the parent or eligible student allows, schools may also disclose, without consent, directory information such as a student's name, address, phone number, date and place of birth, honors and awards, and attendance dates. See www.calstatela.edu/ferpa.

Gramm-Leach-Bliley (GLB) Act: Known as the Financial Modernization Act of 1999, GLB protects the confidentiality and security of consumers' personal financial information held by financial institutions (banks, securities firms, insurance companies, and institutions providing financial services such as processing student loans and payments). To comply, CSULA must establish standards relating to administrative, technical, and physical safeguards.

CA Senate Bill (SB) 1386: Adds CA Civil Code §1798.29 and amends §1798.84 (previously §1798.82) regarding the handling of personal information. Effective 7/1/03, CSULA must notify any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. SB 1386 specifically defines personal information (for a definition, see www.calstatela.edu/its/policies and click on the SB 1386 link).

CA Senate Bill 25: Amends CA Civil Code §1798.85 to limit the use of Social Security Numbers as identifiers.



are you Secure?

QUICK ID THEFT REFERENCE GUIDE



Information Technology Services

INFORMATION SECURITY ASSURANCE

Director, IT Security and Compliance

(323) 343-2600
ITSecurity@calstatela.edu
LIB PW 1070

ITS Help Desk

(323) 343-6170
LIB PW Lobby
helpdesk@calstatela.edu

Are You Secure? Website

www.calstatela.edu/itsecurity

Are You Secure? Quick Reference Guide

[www.calstatela.edu/itsecurity/
quickrefguide.pdf](http://www.calstatela.edu/itsecurity/quickrefguide.pdf)

A guide to protect you and the University

Today, identity theft and fraud are common crimes. They occur quickly, indiscriminately, and may go undetected.

Technology can help us protect confidential information, but technology alone is not enough. Information security assurance uses a two-pronged approach: behavioral and technological, and the campus community should address both equally. Together, both approaches provide the necessary foundation for a safe, secure University environment

Technology, such as firewalls, secure websites, and anti-virus services cannot replace each user's attentiveness and cautious behavior. Students, faculty, and staff are the first line of defense against unauthorized access to information and campus resources. At home and work, we all must protect the information in our computers, notebooks, electronic storage devices, file cabinets, desks, printers, and copiers. We cannot be careless by sharing user IDs and passwords, or by leaving unsecured confidential documents unattended in our offices. We must be cautious about providing confidential information via websites, e-mail, and telephone. And, we all must guard against intruders using social engineering and hacking tactics.

Information security assurance is one of the most important priorities for Cal State L.A. Everyone on campus is responsible for protecting confidential information in whatever format: electronic or printed. The campus appreciates ongoing student, faculty, and staff efforts to help safeguard University information, resources, reputation, and integrity.

Privacy and identity protection are possible only with an informed campus community. Please continue employing best practices and raising your information security awareness. Use this guide to help you protect information – yours and the University's – and to take action if personal or confidential information is at risk. For clarification about what actions to take, contact IT Security and Compliance or the ITS Help Desk.

Peter Quan
Vice President, Information Technology Services
Chief Technology Officer



WHERE CAN I FIND OUT ABOUT INFORMATION SECURITY ASSURANCE?

SECURITY GUIDELINES
www.calstatela.edu/its/policies

Find applicable information technology guidelines; laws and regulations, policies, and Executive Orders.

SECURITY MAILBOX
ITSecurity@calstatela.edu

Submit questions, and report security violations, breaches, vulnerabilities, and issues.

ITS ALERTS
www.calstatela.edu/its/alerts

Subscribe to breaking virus and scam alerts to ensure that appropriate prevention is applied.

ITS NEWS/UPDATES
www.calstatela.edu/its/news

Check this website for announcements, bulletins, and special reports.

HOW DO I PROTECT PERSONAL INFORMATION?

Check Your Mail

Know when to expect bank and credit card statements, and utility and property tax bills. Always deposit outgoing mail in U.S. Mail collection boxes or at your local post office. Never leave outgoing mail in your mailbox. During absences, place a vacation hold on your mail by calling **800-275-8777** or visiting your local post office. If you notice that mail you regularly receive is missing, thieves may have stolen it from your mailbox or had your mail rerouted by fraudulently submitting a change of address to the post office.

If you are a victim:

- Contact the U.S. Postal Inspector and report the crime.
- Locate your local postal inspector at <http://www.usps.com/ncsc/locators/find-is.html>
- Contact your local postmaster to have your mail sent to the proper address.
- Alert your local postal carrier of the problem.

Use Best Information Security Practices

- Never provide personal information over the phone or fax, through the mail, or over the internet unless you initiated the contact with a person or entity you know and trust.
- Never respond to, or click on links in, “phishing” scams – unsolicited e-mail messages that supposedly come from banks, credit unions, payment services, or credit card companies.
- Use a confetti shredder to destroy any document containing personal information, such as cancelled checks, bank statements, medical records, credit applications, utility bills, and expired charge cards.
- Opt out of receiving credit card offers and direct marketing e-mail and telephone calls. Call: **888-567-8688** for information.

Also write:
DMA Opt-Out Preference Service
 PO Box 643; Carmel, NY 10517
www.dmaconsumers.org/privacy.html

WHAT TO DO IF YOUR IDENTITY IS STOLEN

What’s on Your Credit Report?

Your credit report contains your personal information, public records (e.g., liens, bankruptcies), collection accounts (credit cards, loans), credit history, current obligations, credit inquiries, and credit score (rating). This report is used by potential lenders, employers, landlords, and others who want to determine if you have an acceptable credit rating. For a fee, you can order your credit report. If you are an ID theft/fraud victim or have been denied credit, you are entitled to a free report. It is wise to order your report at least once yearly and check that:

- All listed accounts and balances are correct.
- No suspicious activity and only legitimate inquiries for your credit history (e.g., loans/leases you did not apply for) are listed.
- All current and previous residence addresses are correct.
- Your Social Security Number is correct.

Request a report from these credit bureaus:

Equifax 800-685-1111
www.equifax.com

Experian 888-397-3742
www.experian.com

Trans Union 800-888-4213
www.transunion.com



If Your Identity Is Stolen...

- Immediately file a police report and notify the local offices of the FBI, FTC, IRS, and Social Security Administration.
- Immediately contact the fraud departments of the three major credit bureaus.
- Ask that your accounts be flagged with a “fraud alert” requiring creditors to call the credit bureau prior to opening or changing an account.
- Request that fraudulent entries be removed from your accounts.
- Contact recent recipients of your credit report to report errors or fraud.
- Report all suspicious account activity to your creditors.
- Contact creditors where accounts with your name were fraudulently opened.
- Report suspicious investment activity.
- Check if bankruptcy was filed using your identity. If so, notify your creditors.
- Check criminal records/arrests listed with your name.
- Check if driver’s license or identification card fraud occurred.
- Notify utilities, telephone, and trash collection companies that you are an ID theft victim, and that the thief may try to open accounts in your name.
- Notify passport services.
- Keep a detailed record of all actions that you take to resolve your identity theft.

Learn more about identity theft and fraud on the Department of Justice website:
<http://www.usdoj.gov/criminal/fraud/idtheft.html>

HOW DO I PROTECT PERSONAL INFORMATION?

Protect Your Bank Account

Since checks can be replicated and forged, always review all your bank account statements, both checking and savings, for irregularities. Make sure your supply of bank checks is kept in a secure location. Do not order printed checks containing personal confidential information, such as your driver’s license or Social Security Number. Use a confetti shredder to destroy cancelled checks, preprinted deposit slips, and other documents containing bank account information.

If your bank account statement shows suspicious activity:

- Immediately contact your bank.
- Place a stop payment on all outstanding checks.
- Cancel the problem account and open a new one.
- Report fraud to check verification services:
Check Rite 800-766-2748
Telecheck 800-710-9898

Check Your Social Security Earnings and Benefits Statement

Your Earnings and Benefits statement is a record of your Social Security earnings and the estimated resulting benefits you and your family may receive when you are eligible to collect them. Regularly check this statement to see that it is accurate and that no one is illegally using your Social Security Number (SSN) for employment. To order your statement, call **800-722-1213**, or **TTY number: 800-325-0778**, or go to www.ssa.gov.

If your SSN is being used illegally:

- Immediately report misuse to the Social Security Administration (SSA).
- If your situation meets SSA’s fraud victim criteria, the agency will change your SSN.
- To report fraud, contact:
SSA Fraud Hotline 800-269-0271
PO Box 17768
Baltimore, MD 21235
www.ssa.gov/oig/Hotline.htm